REMARKS

The following remarks are responsive to the Final Office Action of January 28, 2009, and the telephone interview conducted on March 12, 2009. Applicants thanks the Examiner for the courtesy shown during the interview.

Claims 1–16 are currently pending in the application. These claims were rejected as follows:

- claims **1 and 11** were rejected under **35 U.S.C. § 112**, first paragraph, as not being enabled;
- claims **1, 2 and 11–13** were rejected under **35 U.S.C. § 102(e)** as being anticipated by **Haukka**, et al. (U.S. Patent Publication No. 2003/0097584); and
- claims **3–10 and 14–16** were rejected under **35 U.S.C. §103(a)** as being obvious over **Haukka** in view of **Hirayama**, et al., U.S. Patent Publication No. 2003/0123434).

Applicants have amended claims 1 and 11 to address the 35 U.S.C. § 112 issue and have made a minor formalities change to claim 14, but otherwise address the final rejection below. Applicants thank the Examiner for indicating that he would enter and consider the above-amendments proposed during the interview after final.

35 U.S.C. § 112, First Paragraph, Claims 1 and 11 Lack of Enablement

1. Applicants have amended independent claims 1 and 11 to restore prior language in place of the language serving as the basis for rejection.

In the Office Action, on pp. 2–3, the Examiner rejected independent claims 1 and 11, indicating that language added by the previous amendment introduced subject matter that was not enabled by the specification.

In response, Applicants have amended independent claims 1 and 11 to remove the language indicated by the Examiner as not being enabled by the Specification. Namely, the language of claim 1 referring to a plurality of extracted parameters has been replaced with

language that was previously in the claim, prior to the last amendment of "at least one parameter." Similarly, with regard to claim 11, the language referring to initiating a set-up of the call, has been replaced with "cause the set-up," as was previously claimed.

Having removed the language indicated by the Examiner has not finding support in the Specification, Applicants respectfully request that the Examiner withdraw the 35 U.S.C. § 112 rejection from the application.

35 U.S.C. § 103(a), Claims 1, 2 and 11–13 Anticipation by Haukka

2. Haukka fails to teach a remote call manager server decrypting a control code, comparing a parameter extracted from the decrypted control code, and setting up a call as a function of the comparison.

In the Final Office Action, on pp. 4–5, the Examiner rejected claims 1, 2, and 11–13 as being anticipated by Haukka.

Focusing on the claimed control code, Applicants note that the Examiner has equated Haukka's control code as follows.

The Examiner indicated that Haukka discloses the claimed "control code" in a number of places: ¶ 0009:1–4, 8, 9 (<paragraph no.>:<lines>); ¶ 0023:5–7; and ¶ 0017:23–26.

These respective portions of Haukka are reproduced below.

¶ 0009:1–4, 8, 9:

> [0009] Once the temporary identity index is created, it may be inserted in a header of the message. For example, the temporary identity index may be inserted in a call-info header field of a session initiation protocol (SIP) message in place of a request Uniform Resource Identifier (URI) for providing the sender's identity. When the SIP message is to be sent, the sender first generates the SIP message which is then encrypted using an encryption algorithm determined during registration of the user equipment.

¶ 0017:23–26:

> [0017] ...Both the P-CSCF 20 and the UE 10 then calculate a temporary identity index using a hash function Hk(x), where x

> is a public identity of the UE 10, and k is one of the private keys CK and IK.

and

¶ 0023:5–7

> However, other identification parameters could also be encrypted with the message and inserted in a header as required by a specific message.

These sections do not teach or suggest a control code, as presently claimed by the independent claims.

Claim 1 requires:

> inserting into a field of a call set-up request frame an encrypted control code containing parameters relating to the identity of a telecommunications terminal from which the telephone call is sent;

With reference to ¶ 0009, if the Examiner intends that the session initiation protocol (SIP) message would read on the claimed control code (and the Examiner is not entirely clear on this point), then Haukka does not teach using the SIP message itself to control anything, let alone the identity of the sender of this SIP message. If the Examiner intends that the "temporary identity index" of ¶ 0009 to read on the claimed control code, then Applicants address this interpretation in the immediately following paragraph. The Examiner is respectfully requested to clearly specify which element of Haukka is being equated to the claimed control code.

With reference to ¶ 0017, the Examiner intends that the "temporary identity index" would read on the claimed control code. However, in Haukka, this identity index is used as such by the "network element" (receiver of the message), and not used after being decrypted.

Claim 1 requires:

> decrypting, at a remote call management server, the encrypted control code;
>
> comparing at least one parameter extracted from the decrypted control code with corresponding information stored in a database hosted in the management server; and
>
> setting up the call as a function of the result of said comparison.

Thus, claim 1 requires that the control code be used after being decrypted by the receiver.

But Haukka does not even refer to a decryption of the temporary identity index because the temporary identity index is used as a hash value, not as an encrypted value to begin with. Haukka states:

> Both the P-CSCF 20 and the UE 10 then calculate a temporary identity index using a hash function Hk(x), where x is a public identity of the UE 10, and k is one of the private keys CK and IK. (¶ 0017)
>
> ...
>
> The calculation, using the has function, produces an ID string (i.e., the temporary identity index) which is saved as part of the security suite at the UE 10 and P-CSCF 20.

The hash function value, and hence Haukka's temporary identity index, cannot be equated with the presently claimed encrypted and decrypted control code because that is not how a hash function works. A hash function value is a numeric value that is easy to create from a set of data, but extremely hard mathematically to replicate with a different set of data. It is impossible to "decrypt" the hash function to recover the original data. In other words, Haukka utilizes hash functions that are not decrypted or decryptable.

Finally, with reference to ¶ 0023, the Examiner intends that the sender's Uniform Resource Identifier (URI) would read on the claimed control code. However, Haukka does not explicitly disclose that the encrypted URI is decrypted by the network element. Even if one considered arguendo that Haukka implicitly discloses that the encrypted URI is decrypted by the network element (in order to identify the sender of the SIP message), one would find no motivation in Haukka for "comparing [the URI] extracted from the decrypted control code with corresponding information stored in a database," since the URI constitutes by itself enough information for identifying the sender, and thus there would be no motivation for including extraneous information.

Furthermore, one would find no motivation in Haukka for "setting up the call as a function of the result of said comparison," since Haukka only teaches (see ¶ 0004) that "to initiate or establish a session, an SIP message is generated at a user's equipment and is sent to the intended recipient via a communication network".

In sum, Haukka does not teach a method of "verifying the identity of the sender", but rather teaches a method of protecting the confidentiality of the sender.

Haukka states:

> [0006] It is an object of the present invention **to provide confidentiality protection** in messages sent from a user equipment (UE) to a network element in a communication network with which the UE is in direct communication.
>
> [0007] According to a first embodiment of the present invention, **a method for confidentiality protection** includes creating a temporary identity index and associating this index with a sender-receiver pair, i.e., the UE and the network element. The temporary identity index is created using a secret key and an algorithm known to the sender and receiver and public information identifying the sender of the message. [emphasis added]

In Haukka, the sender is identified by the network element by means of the temporary identity index, but this relates to confidentiality protection, and not to identity verification—and simpler ways in the art exist for verifying the identity of a sender.

Haukka does not teach or suggest the element of "a remote call management server decrypting the control code." Haukka does not teach or suggest the element of of "comparing at least one parameter extracted from the decrypted control code." Haukka does not teach or suggest the element of "setting up the call as a function of the result of said comparison." As a result Haukka cannot advantageously achieve using the SIP message to establish an Internet session call between the calling and called parties after the successful validation of SIP security parameters.

For these reasons, independent claims 1 and 11 are not anticipated by Haukka, and dependent claims 2, 12, and 13 are not anticipated by Haukka by virtue of their dependence from claims 1 and 11 respectively.

35 U.S.C. §103(a) Obviousness of Claims 3–10 and 14–16 over Haukka in View of Hirayama

3. Applicants rely upon the above arguments with respect to the remaining dependent claims, and assert that the addition of Hirayama fails to supplant the deficiencies identified above with respect to Haukka.

In the Office Action, on pp. 5–7, the Examiner combined Haukka with Hirayama in establishing an obviating combination of references for various dependent claims in the present application. Without addressing the specifics of the additional references on the merits, except for the arguments presented below, Applicants rely upon the above arguments and assert that the disclosure of Hirayama, alone or in combination, does not serve to solve the deficiencies of the Haukka reference. The Examiner has cited this reference for purposes related to the specifics of the dependent claims.

With respect to claims 6 and 9, the combination of Haukka and Hirayama is ineffective since Haukka does not disclose a step of using a decrypted control code for comparison with corresponding information stored in a database, and Hirayama does not cure this defect.

4. The combination of Haukka and Hirayama fails to teach or suggest a database that includes an address identifying the telecommunications terminal, as required by claims 3 and 4.

In the Office Action, on pp. 6 and 7, the Examiner rejected claims 3 and 4 as being obvious over the disclosure of Haukka and Hirayama. The Examiner stated:

> As per claim 3, Haukka as modified teaches the information stored in the database includes [sic] an address identifying the terminal (Haukka: Para [0023] Line 5–7 and Para [0009] Line 7–9) & (Hirayama: Para [0002]). See the same rationale of combination applied herein as above in rejecting the claim 6.
>
> As per claim 4, Haukka as modified teaches the said information is transferred from the terminal to the database during a first call sent by the terminal (Haukka: Para [0023] Line 5–7 and Para [0009] Line 7–9).

Applicants note, however, that there is no disclosure in either of these references to a database that includes an address identifying the telecommunications terminal, and the word "database" nor any equivalent structure is used. In the event that this rejection is maintained, Applicants respectfully request that the Examiner identify with specificity which reference discloses the claimed database and which disclosed element in these references reads on the claimed database.

For these reasons, the Applicants assert that the claim language clearly distinguishes over the prior art, and respectfully request that the Examiner withdraw the § 103 rejection from the present application.

CONCLUSION

For the foregoing reasons, all pending claims in the present application are believed to be allowable. Thus, the application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Req. No. 35,665
Mark Bergner, Reg. No. 45,877
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: March 25, 2009
CH01/ 25318479.2